

NOV 16 2006

Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)  
Approved for use through xx/xx/200x. OMB 0651-000x  
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE  
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>PRE-APPEAL BRIEF REQUEST FOR REVIEW</b>		Docket Number (Optional) NAI1P461/01.119.01	
I hereby certify that this correspondence is being transmitted via facsimile to the Commissioner for Patents, Alexandria, VA 22313-1450 to fax number (571) 273-8300. on <b>November 16, 2006</b> Signature <u><i>April Skovmand</i></u> Typed or printed name <u>April Skovmand</u>		Application Number <b>10/036,521</b>	Filed <b>01/07/2002</b>
		First Named Inventor <b>Robert John Ackroyd</b>	
		Art Unit <b>2136</b>	Examiner <b>Shiferaw, Eleni A.</b>
Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.			
This request is being filed with a notice of appeal.			
The review is requested for the reason(s) stated on the attached sheet(s). Note: No more than five (5) pages may be provided.			
I am the		Signature <u><i>Kevin J. Zilka</i></u>	
<input type="checkbox"/> applicant/inventor.		Typed or printed name <b>Kevin J. Zilka</b>	
<input type="checkbox"/> assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)		Telephone number <b>408-971-2573</b>	
<input checked="" type="checkbox"/> attorney or agent of record. <b>41,429</b> Registration number		Date <b>11/16/06</b>	
<input type="checkbox"/> attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34			
NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.			
<input checked="" type="checkbox"/> Total of <u>1</u> forms are submitted.			

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

-1-

REMARKS

The Examiner has rejected Claims 1-3, 6-12, 15-21, and 24-27 under 35 U.S.C. 102(e) as being anticipated by Schertz et al. (U.S. Publication No. 2003/0084322 A1). Applicant respectfully disagrees with such rejection.

With respect to each of the independent claims, the Examiner has relied on paragraphs [0018], [0021], [0023], and [0030] from the Schertz reference to make a prior art showing of applicant's claimed "detecting from said plurality of log data messages received by said managing computer a pattern and a network-wide threshold of malware detection across said plurality of network connected computers matching at least one predetermined trigger" (see this or similar, but not necessarily identical language in each of the independent claims).

Applicant respectfully asserts that the excerpts from Schertz relied on by the Examiner merely teach a method of performing network-based intrusion detection on packets inbound from the internet via a firewall or proxy server destined for a device or multiple devices on the network. In addition, the excerpts teach that "[n]etwork-based intrusion protection systems analyze data inbound from the Internet and collects network packets to compare against a data base of various known attack signatures or bit patterns." In sharp contrast, applicant claims "detecting from said plurality of log data messages received by said managing computer a pattern and a network-wide threshold of malware detection across said plurality of network connected computers matching at least one predetermined trigger" (emphasis added), in the context claimed.

In the Office Action dated 07/26/06, the Examiner has argued that "Schertz et al. teaches virus intrusion detecting/monitoring/scanning of ALL devices on a network network-wide, [that] network-based virus intrusion detection system typically monitors all network activity and network traffic, [and that] Network-based virus intrusion protection systems analyze data inbound from the internet and collects network packets to compare against a database of various known attack signatures or bit patterns."

-2-

Applicant respectfully disagrees, and asserts that merely detecting, monitoring and scanning all network activity, as the Examiner has noted, fails to even suggest any sort of network-wide threshold, in the manner claimed by applicant. In addition, simply disclosing comparing network packets against a database of various known attack signature, as also noted by the Examiner, does not specifically meet a “network-wide threshold of malware detection across said plurality of network connected computers,” as applicant claims (emphasis added).

With respect to each of the independent claims, the Examiner has also relied on paragraphs [0003] and [0018] from the Shertz reference to make a prior art showing of applicant’s claimed “network-wide threshold being applied to a sum of detections, the detections each being associated with a different one of the network connected computers” (see this or similar, but not necessarily identical language in each of the independent claims).

Applicant respectfully points out that the excerpts from Shertz relied on by the Examiner merely disclose that “[a] network-based system typically monitors all network activity and network traffic” (paragraph [0003]) and that “[n]etwork-based intrusion protection systems analyze data inbound from the Internet and collects network packets to compare against a data base of various known attack signatures or bit patterns” (paragraph [0018]-emphasis added). Applicant respectfully asserts that simply “collect[ing] network packets to compare against a data base,” as in Shertz, does not teach applying a “network-wide threshold” to “a sum of detections,” let alone where such detections are each “associated with a different one of the network connected computers,” as claimed by applicant (emphasis added).

Additionally, the Examiner has rejected Claims 1, 10, and 19 under 35 U.S.C. 102(e) as being anticipated by Chefalas et al (U.S. Publication No. 2002/0116639 A1). Applicant respectfully disagrees with such rejection.

-3-

With respect to each of the independent claims, the Examiner has relied on paragraph [0012], Fig. 4A-B, and Fig. 5A-B from the Chefalas reference to make a prior art showing of applicant's claimed "pattern and a network-wide threshold of malware detection across said plurality of network connected computers matching at least one predetermined trigger" (see this or similar, but not necessarily identical language in each of the independent claims).

Applicant respectfully asserts that such excerpts merely teach that "[i]n response to detecting a virus infection, the VSN at the client data processing system sends notification of a presence of the virus on the data processing system to a software module known as the virus scanner controller (VSC) residing at a server, wherein the notification includes an identification of an action taken in response to detecting the virus" and that "the server data processing system may execute an action based on a business policy in response to receiving the notification" (emphasis added). Additionally, the figures relied upon by the Examiner simply illustrate "business events" and "illustrations of policies for taking action in response to notification of a virus."

Applicant respectfully asserts that merely "detecting a virus infection," sending "notification of a presence of the virus" as well as "an action taken in response to detecting the virus," and executing "an action based on a business policy," as in Chefalas, does not teach any sort of threshold, let alone a "pattern and a network-wide threshold of malware detection across said plurality of network connected computers matching at least one predetermined trigger," as claimed by applicant (emphasis added).

Additionally, with respect to each of the independent claims, the Examiner has relied on paragraphs [0012], [0022]-[0024], and [0057]-[0058] from the Chefalas reference to make a prior art showing of applicant's claimed "network-wide threshold being applied to a sum of detections, the detections each being associated with a different one of the network connected computers" (see this or similar, but not necessarily identical language in each of the independent claims).

-4-

Applicant respectfully points out that the excerpts relied on by the Examiner merely teach that “the VSN at the client data processing system sends notification of a presence of the virus on the data processing system to a software module” (paragraph [0012]) and that “the business event is compared to policy... [and] an action is initiated based on the comparison” (paragraph [0058]-emphasis added). Such excerpts also teach that the “[n]etwork data processing system 100 is a network of computers in which the present invention may be implemented” (emphasis added). However, merely disclosing the “presence of the virus” on a network and comparing a “business event” to a “policy,” as in Chefalas, does not teach the use of a “network-wide threshold” or a “sum of detections,” much less a “network-wide threshold being applied to a sum of detections, the detections each being associated with a different one of the network connected computers,” as claimed by applicant (emphasis added).

Also, the Examiner has rejected Claims 1, 10, and 19 under 35 U.S.C. 102(e) as being anticipated by Hypponen et al (U.S. Publication No. 2003/0191957 A1). Applicant respectfully disagrees with such rejection.

With respect to each of the independent claims, the Examiner has relied on paragraphs [0035] and [0036], as well as Fig. 1 from the Hypponen reference to make a prior art showing of applicant’s claimed “detecting from said plurality of log data messages received by said managing computer a pattern and a network-wide threshold of malware detection across said plurality of network connected computers matching at least one predetermined trigger, the network-wide threshold being applied to a sum of detections, the detections each being associated with a different one of the network connected computers” (see this or similar, but not necessarily identical language in each of the independent claims).

Applicant respectfully asserts that such excerpts from Hypponen merely teach that “[t]he agent’s function is to intercept data which is being transferred through the [protected] system 4 on which the agent is running...[and that t]he intercepted data is scanned on-the-fly by the agent to determine whether or not the data has a form which

-5-

may contain a virus" (paragraph [0035]-emphasis added). Such excerpts also teach that "any data which is identified by the agent as being suspect, is re-routed over the network 1, from the protected system in question, to the virus scanning server 7...[and that u]pon receipt of the suspect data, the server 7 scans the data for viruses" (paragraph [0035]-emphasis added).

Applicant respectfully asserts that there is simply no disclosure in the excerpts relied on by the Examiner of "a pattern and a network-wide threshold of malware detection" (emphasis added), as claimed by applicant. For example, "intercept[ing] data which is being transferred through the [protected] system," "scan[ing] on-the-fly by the agent" for viruses, and re-routing suspect data "to the virus scanning server," as in Hypponen, does not meet any sort of a "threshold" or "a sum of detections," much less a "network-wide threshold being applied to a sum of detections, the detections each being associated with a different one of the network connected computers," as applicant specifically claims (emphasis added).

In the Office Action mailed 7/26/2006, the Examiner has argued that Hypponen "teaches a virus scanning server 7 scanning and detecting the received suspicious log data using F-PROT TM, and F-SECURE TM, and/or detecting virus on a network-wide connected computer" where "[d]etected/suspected data packets...are compared with known virus signature." Applicant respectfully asserts that merely detecting viruses on a network connected computer, as the Examiner notes, does not even suggest any sort of threshold, let alone "a network-wide threshold of malware detection across said plurality of network connected computers," as applicant specifically claims (emphasis added). Moreover, simply nowhere in Hypponen is there any disclosure of a sum of detections, as applicant claims.